

REMARKS

The Office Action dated June 25, 2008 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-35 are currently pending in the present application, including independent claims 1, 10, 14, 17, and 20-26. Specifically, Applicants here amend claims 2, 5-6, 8-10, 12, 15, 17, 18, and 22-23 and add new claims 24-35 to more particularly point out and distinctly claim the subject matter that the Applicants regard is the invention. Entry of the claim amendments and additions is respectfully requested because no new matter is being added. It is believed that that all of the pending rejections are addressed below, and all of the pending claims are in condition for allowance in view of the amendments and the following comments. Claims 1-35 are hereby submitted for consideration.

Claim Allowances

Applicants wish to express great appreciated for the indication given in the Office Action that claims 1-16 and 20-22 are allowed. Although claims 2, 5-6, 8-10, 12, 15, and 22 are currently amended, Applicants urge that these amendments serve only to clarify the subject matter of recited embodiments of the present invention and would not impact the reasons for allowability as provide in the Office Action. Therefore, Applicants urge that claims 1-16 and 20-22 continue to be allowable for at least the reasons provided in the Office Action. Applicants further have added new claims 24-35, and these claims should be

allowable on a similar basis as allowed claims 1-16 and 20-22. For example, claim 24-26 although patentably distinct, recite similar limitations, respectively, to allowed claims 1, 14, and 21. Applicants respectfully note that the components disclosed in the present application, such as the home agent, foreign agent, and the terminal of FIG. 2 include software components according to the applicable technical standards. Moreover, Applicants note that as depicted in transmission packet of FIG. 4 and the process flow of FIG. 5, the disclosed methods may be software implemented. Likewise, new claims 27-35 depend from one of the allowed claims 20 and 21, and should be allowed for at least this reason, as well as for the limitations separately recited in these claims.

Rejection under 35 U.S.C. §102(b)

Claims 17-19 and 23 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,311,596 (Robert). The rejection is traversed as being based on a reference that does not teach or suggest each of the elements of claims 17-19 and 23.

Independent Claim 17, upon which claims 18 and 19 depend, relates a method that includes receiving a set of challenges from a telecommunications network, wherein each one of the challenges is contained in an authentication data block comprising said one of said challenges, a response and a key. One challenge is chosen from the set of challenges, and a response and a key are determined based on the chosen challenge. An authenticator is determined based on the key corresponding to the chosen challenge. The authenticator and a data unit are transmitted to the telecommunications network, such that the data unit relates to the manner in which the authenticator is formed. The method of

claim 17 further includes notifying the telecommunications network of which challenge was chosen, such that a check value is determined with the key corresponding to the chosen challenge, and this check value is compared with the authenticator.

Independent claim 23 relates to an apparatus that includes receiving means for receiving a set of challenges from a telecommunications network, wherein each one of the challenges is contained in an authentication data block comprising said one of said challenges, a response and a key. The apparatus of claim 23 includes choosing means for choosing one challenge from the set of challenges and determining means for determining a response and a key based on the chosen challenge. The apparatus of claim 23 further includes determining means for determining an authenticator based on the key corresponding to the chosen challenge, and transmitting means for transmitting said authenticator and a data unit to the telecommunications network, said data unit relating to the manner in which the authenticator is formed. Also, notifying means in the apparatus of claim 23 are for notifying the telecommunications network of which challenge was chosen, such that a check value is determined with the key corresponding to the chosen challenge, and this check value is compared with the authenticator.

As outlined below, Robert does not teach or suggest each of the elements of the pending claims.

Robert discloses an authentication method where an answering modem provides a user transparent re-authentication of an originating modem via a challenge/response protocol. In particular, after establishing the data connection with the originating modem, a CPU sends a request to the originating modem for its modem identification (ID)

number. The modem ID number is a predetermined number assigned to the originating modem. If the CPU does not receive the originating modem's ID number, the CPU sends an "access denied" message and drops the data connection. However, if the CPU receives the originating modem's ID number, the CPU retrieves a corresponding data encryption key from a key list. The key list is a previously stored list, in a memory, which includes a plurality of modem ID numbers, each of which represents a possible originating modem, where each modem ID number is associated with a data encryption key. This associated data encryption key, like the modem ID, is also pre-determined in the originating modem.

Robert also discloses that after retrieving the associated data encryption key for the originating modem, the CPU randomly generates a number, which is known as a challenge. This challenge is sent to the originating modem, and upon receipt of the challenge the originating modem encrypts the challenge to generate a response, that is, a form of "cipher text," which is sent back to answering modem. The encryption performed by the originating modem uses the stored data encryption key.

Robert further discloses that if the CPU does not receive a response from the originating modem, the CPU sends an "access denied" message and drops the data connection. However, if the CPU receives a response, the CPU decrypts the response using the associated data encryption key and verifies the identity of originating modem. If the decrypted response and the challenge do not match, the CPU sends an "access denied" message and interrupts the data connection. However, if the CPU verifies the identity of the originating modem, that is, if the decrypted response and the challenge

match, the CPU does not disturb the data connection and checks if this is the completion of the first re-authentication attempt. If this is the completion of the first re-authentication attempt, the CPU enables the transfer of data information between answering modem and the originating modem. Once the data transfer is enabled, for subsequent re-authentication attempts, the CPU sets an interrupt for a predetermined period of time, T. After the period of time, T, passes, the CPU re-authenticates the data connection. This re-authentication process continues for the duration of the data connection. See at least Figure 3 and Col. 4, line 32-Col. 5, line 44.

Applicant submits that Robert does not teach or suggest each of the elements of claims 17-19 and 23. Each of independent claims 17 and 23, in part, recites receiving a set of challenges from a telecommunications network and choosing one challenge from the set of challenges. Each of the challenges is contained in an authentication data block comprising a challenges, a response and a key. Each of independent claims 17 and 23 also recites determining a response and a key based on the chosen challenge and determining an authenticator based on the key corresponding to the chosen challenge. Each of independent claims 17 and 23 further recites transmitting the authenticator and a data unit to the telecommunications network, wherein the data unit relates to the manner in which the authenticator is formed and notifying the network of the chosen challenge, such that a check value is determined with the key corresponding to the chosen challenge, and this check value is compared with the authenticator. Robert does not teach or suggest these features.

As noted above, Col. 5, lines 24-31 of Robert discloses that re-authentication, and hence the necessity to issue another challenge, only happens after a time, T. In the intervening period in Robert, the data connection is allowed to be maintained. Consequently, there is no teaching or suggestion in Robert of choosing one challenge from the set of challenges, as recited in the pending claims. Instead, in Robert, only one random number challenge is sent at a time.

Robert further discloses in Col. 4, lines 49-55 that a key is retrieved based on the modem ID. Therefore, there is no teaching or suggestion in Robert of determining a response and a key based on the chosen challenge, as recited in claims 17, 21 and 23. Apart from the fact that Robert does not teach or suggest choosing a challenge, in Robert the key is not determined based on any challenge, but is determined based only on the ID of the calling modem.

Furthermore, Robert does not teach or suggest transmitting the authenticator and a data unit to the telecommunications network, wherein the data unit relates to the manner in which the authenticator is formed, as recited in claims 17, 21 and 23. Col. 5, lines 23-24 of Robert merely discloses that data transfer is enabled following re-authentication. Robert is silent as to the nature of what, if anything, is transmitted to the network and certainly does not teach or suggest transmission of a data unit relating to the manner in which the authenticator is formed, as recited in the pending claims. There is also no teaching or suggestion in Robert of notifying the network of the chosen challenge, as recited in claims 17, 21 and 23.

Based on the distinctions noted above, Applicant requests that the rejection under 35 U.S.C. 102(b) be withdrawn because Robert does not teach or suggest each of the elements of claims 17 and 23. Claims 18-19 depend on claim 17 and should also be allowed because of their dependence on claim 17, in addition to the further limitations recited in claims 18 and 19.

Claims 17-19 and 23 were rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent Publication No. 2002/0069174 (Fox). The rejection is traversed as being based on a reference that does not teach or suggest each of the elements of claims 17-19 and 23.

Fox is directed to a method for providing a standardized and interoperable protocol for facilitating electronic transactions between parties by building on well known protocols. Specifically, Fox provides a GUMP Registration Meta-Protocol (GRMP) framework for designing and implementing a financial institution's certification policies to produce a client's Certified Public Signature Key (CPSK), packaged as a GUMP Relationship Certificate (GRC). The GRMP framework includes the following steps. The client applies for a certificate either in person or through the financial institution's web site. The client provides satisfactory proof of identity to the official of the institution. In the case of face-to-face certification, identification might be showing government documents. In the case of electronic identification, the institution might require a signature on a challenge with a verification key from a generic identity certificate, such as one from VeriSign Inc. The official of the institution gives the client a one-time secret (OTS) out-of-band, for example, in a PIN mailer. The client digitally

signs and submits a Request for Certification (RFCert), which contains a proposed public signature key, and securely proves possession of the OTS. The institution digitally signs and sends back a GRC binding the client's public signature key to the OTS.

Applicant submits that Fox does not teach or suggest each of the elements of claims 17-19 and 23. Each of independent claims 17 and 23, in part, recites receiving a set of challenges from a telecommunications network and choosing one challenge from the set of challenges. Each of the challenges is contained in an authentication data block comprising a challenges, a response and a key. Each of independent claims 17 and 23 also recites determining a response and a key based on the chosen challenge and determining an authenticator based on the key corresponding to the chosen challenge. Each of independent claims 17 and 23 further recites transmitting the authenticator and a data unit to the telecommunications network, wherein the data unit relates to the manner in which the authenticator is formed and notifying the network of the chosen challenge such that a check value is determined with the key corresponding to the chosen challenge, and this check value is compared with the authenticator. . Fox does not teach or suggest these features.

Fox discloses a method for performing electronic commerce transactions, as stated in the Abstract and in paragraph 0002. Thus, it is to be noted that Fox is not implemented in a telecommunications network as disclosed in the present application. As disclosed in paragraph 0009 of Fox, a first party applies for registration with a second party (e.g. a financial institution) to enable the first party to have access to financial resources through the second party. Fox discloses that when making the request, the first party transmits a proof

of identity. Having confirmed the first party's identity, Fox discloses that the second party returns a digitally signed certificate which includes the transmitted proof of identity. Thus, Fox discloses that an index to the resources available is provided to the first party. This certificate enables payment to be made for goods used by the first party.

Paragraph 0076 of Fox refers to "a challenge" but there is no teaching or suggestion in Fox of the parties receiving of a set of challenges from a telecommunications network or of choosing one of the set of challenges, as recited in claims 17 and 23. There is also no teaching or suggestion in Fox of determining a response and a key based on the chosen challenge, as recited in claims 17 and 23. This is because no challenge is chosen and also because Fox uses what it describes as public and private keys. Paragraphs 0010 and 0012 of Fox disclose that both these keys are associated with the digital signature of the first party. This contrasts with the inventive feature of choosing a key based on a chosen challenge. There is also no teaching or suggestion in Fox of notifying a telecommunications network of the chosen challenge.

Based on the distinctions noted above, Applicant requests that the rejection under 35 U.S.C. 102(e) be withdrawn because Fox does not teach or suggest each of the elements of claims 17 and 23. Claims 18-19 depend on claim 17 and should also be allowed because of their dependence on claim 17, in addition to the further limitations recited in claims 18 and 19.

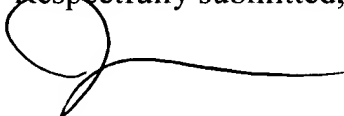
As noted above, Applicant submits that each of claims 17-19 and 23 recite subject matter that is neither disclosed nor suggested by the cited reference. Applicants

respectfully request that all of claims 17-19, 23, and 24-35 be allowed, claims 1-16 and 20-22 continue to be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



David D. Nelson
Registration No. 47,818

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

DDN/sjm
Enclosures: RCE Transmittal
Additional Claims Transmittal
Check No. 19621